Quantum key distribution using quantum Faraday rotators

Taeseung Choi and Mahn-Soo Choi*

Department of Physics, Korea University, Seoul 136-713, Korea

(Dated: February 9, 2008)

Abstract

We propose a new quantum key distribution (QKD) protocol based on the fully quantum mechanical states of the Faraday rotators. The protocol is unconditionally secure against collective attacks for multi-photon source up to two photons on a noisy environment. It is also robust against impersonation attacks. The protocol may be implemented experimentally with the current spintronics technology on semiconductors.

PACS numbers: 03.67.Dd, 03.65.Nk

*Electronic address: choims@korea.ac.kr

I. INTRODUCTION

The computational algorithm powered by quantum mechanics, on the one hand, has posed a serious threat to the classical cryptosystem[1]. On the other hand, quantum cryptography allows for secure sharing of private keys. Ever since the pioneering works by Bennet, Brassard, and Ekert[2, 3, 4], a great number of new quantum key distribution (QKD) protocols have been proposed to enhance the security and efficiency under non-idealistic situations and to incorporate new ideas[5]. In particular, Boström and Felbinger[6] recently proposed the so-called *ping-pong protocol*. The protocol is interesting in that it enables direct communication deterministically and without classical communications (except for checking eavesdropping). Although the original protocol turned out to be insecure in the case of lossy channels[7] and against blind attacks without eavesdropping[8], the idea still survives in a recent modified version[9].

In the ping-pong protocol[6, 9], Bob sends a qubit to Alice, Alice performs a unitary operation on it with a random probability p and send it back to Bob, and finally Bob make a measurement on it. The unitary operation by Alice (if ever performed) transforms the initial state of the qubit to a state orthogonal to the initial state. This enables Bob to read Alice's massage directly. Putting another way, the unitary operation is performed conditioned on the *classical* information (0 or 1) that Alice wants to send to Bob. A conceptually interesting question would be, "What if we perform the unitary operation conditioned on the *quantum state* of another qubit?" In this work, we propose a new QKD protocol implementing this idea and address the security issues of it. The protocol is explained in Section II. We will show in Sections III and IV that the protocol is secure against eavesdropping for ideal single-photon source and robust against impersonation attacks. The protocol turns out to be insecure when the photon source produces more than two photons; this will be analyzed in Section V. We will discuss in Section VI possible experimental realizations of the protocol using semiconductor spintronics.

II. PROTOCOL

While the protocol is independent of the physical system in use, we will have in mind the photon polarizations as travel qubits and electron spins as home qubits. In the description

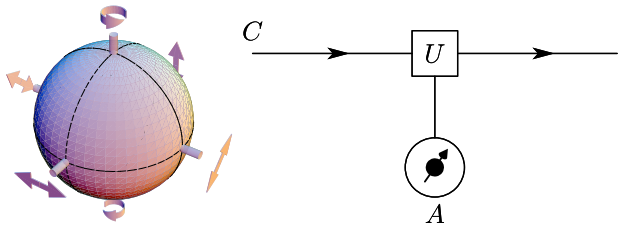

FIG. 1: (color on-line) (a) Poincaré sphere for photon polarization or Bloch sphere for spin. (b) Quantum Faraday rotation (QFR) or conditional rotation $U_{A;C}$ on C conditioned by A; see Eq. (2). It rotates the state of qubit C around z-axis by angle $\pm\pi/2$ depending on the state of qubit A.

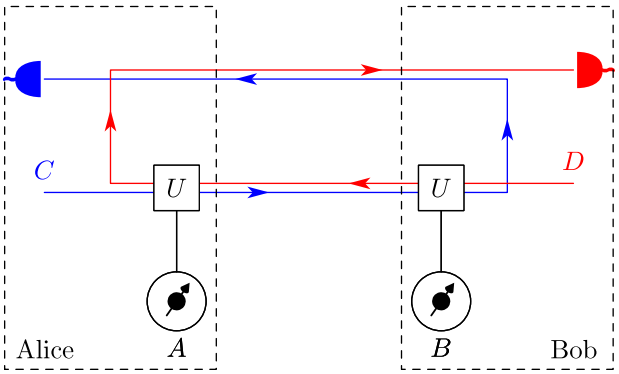

FIG. 2: (color on-line) Quantum key distribution protocol using quantum Faraday rotators.

of the protocol, we will use as the basis the eigenstates of σ^z, $|\uparrow\rangle$ (right-handed circular polarization) and $|\downarrow\rangle$ (left-handed circular polarization). We denote by $|\phi\rangle$ the state along the azimuthal angle ϕ on the equator of the Poincaré (or Bloch) sphere:

$$|\phi\rangle = \frac{|\uparrow\rangle + e^{+i\phi}\,|\downarrow\rangle}{\sqrt{2}}\,. \tag{1}$$

The key element of our protocol will be the *quantum Faraday rotation* (QFR), namely, the Faraday rotation by angle $\pi/2$ around z-axis of the Poincaré sphere

$$U_{A;C} = \exp\left[-i(\pi/4)\sigma_A^z\sigma_C^z\right] \tag{2}$$

on the travel qubit C *conditioned by* the home qubit A. For example, operating on the product state $|\phi=0\rangle_A\,|\phi\rangle_C$, it gives

$$U_{A;C}\,|0\rangle_A\,|\phi\rangle_C = \frac{e^{-i\pi/4}\,|\uparrow\rangle_A\,|\phi_+\rangle_C + e^{+i\pi/4}\,|\downarrow\rangle_A\,|\phi_-\rangle_C}{\sqrt{2}}, \tag{3}$$

where $|\phi_\pm\rangle = |\phi \pm \pi/2\rangle$. In the quantum information theoretic terms, the QFR in Eq. (2) corresponds to the *conditional phase shift*. Possible physical realizations of QFR will be discussed later.

The protocol is as following. (1) To start the nth iteration of the protocol, Alice and Bob first prepare their home qubits A and B, respectively, in the state $|\phi = 0\rangle$[10]. (2) Alice then takes a travel qubit C and prepares it in the state $|\alpha\rangle$. The angle α should be chosen randomly in the interval $0 \leq \alpha < 2\pi$. (3) Alice performs (by interacting A and C) the QFR $U_{A;C}$ on C and send it to Bob. We note that on its way to Bob, the travel qubit C is maximally entangled with A:

$$e^{-i\pi/4} |\uparrow\rangle_A |\alpha_+\rangle_C + e^{+i\pi/4} |\downarrow\rangle_A |\alpha_-\rangle_C \tag{4}$$

(not normalized). (4) Bob receives C, performs $U_{B;C}$ on it, and send it back to Alice. The qubit C is again maximally entangled on its way back to Alice, now with both A and B :

$$(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)_{AB} |\alpha\rangle_C - i\,(|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle)_{AB} |\bar{\alpha}\rangle_C \tag{5}$$

(not normalized), where $|\bar{\alpha}\rangle \equiv |\alpha + \pi\rangle$. (5) Now Bob takes his own travel qubit D and prepares it in the state $|\beta\rangle$. The angle β should be chosen randomly in the interval $0 \leq \beta < 2\pi$. (6) Bob performs the QFR $U_{B;D}$ on D and send it to Alice. (7) Alice receives D, performs $U_{A;D}$ on it, and send it back to Bob. The final state of all the qubits A, B, C, and D is given by a GHZ-like state

$$(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)_{AB} |\alpha\beta\rangle_{CD} - (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)_{AB} |\bar{\alpha}\bar{\beta}\rangle_{CD} \tag{6}$$

(8) Alice measures the observable $S_\alpha = \cos\alpha\sigma^x + \sin\alpha\sigma^y$ on C. Likewise, Bob measures the observable $S_\beta = \cos\beta\sigma^x + \sin\beta\sigma^y$ on D. They will get (in the ideal case) the identical result $+1$ or -1, which enables Alice and Bob to share the the key $K_{2n-1} = 1$ or 0. (9) If $K_{2n-1} = 1$, Bob performs σ^x (the NOT gate), on his home qubit B. (10) Alice and Bob measures σ^z on their home qubits A and B, respectively. Depending on the measurement result, another bit of key $K_{2n} = 0$ ($\sigma^x = +1$) or 1 ($\sigma^x = -1$) is generated. (11) Repeat the steps 1 through 10 with n increased by 1 until n becomes N. (12) Alice and Bob takes randomly M bits out of $\{K_{2k-1} | k = 1, \cdots, N\}$, and test possible eavesdropping (or any other attack) by comparing the values through a classical communication channel.

A few remarks on the procedure are in order. Alice can measure S_α (see Step 8 above) even before the Step 5. It follows from the GHZ-like structure of the states in Eqs. (5) and (6). Step 9 is not essential. It can be removed with a minor change in Step 10.

Before analyzing the security of the protocol, we point out a few interesting features of the protocol. First, the travel qubit is always in a maximally entangled states with the home

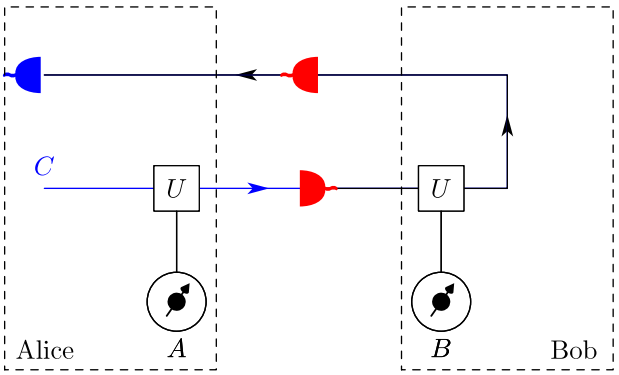

FIG. 3: (color on-line) General attack on a noisy environment.

qubit(s) whenever exposed to eavesdropping. This is the essential feature of the protocol that provides the protocol with the security. Second, at the key sharing stage no classical communication is necessary. The key is shared only through the quantum channel[11]. This is also closely related to the security of the protocol. Third, two bits are generated out of one iteration and they have the common security fate. If the first bit has been tampered by eavesdropping or noise in the channel, the security of the second bit is not guaranteed either.

III. SECURITY PROOF

Let us analyze general attacks from a third party in case the photon source generates single photon. We closely follow the lines in Ref.[9]. As usual, Eve is assumed to be an almighty eavesdropper limited only by the law of physics. The most general (assuming that Eve does not know Alice's choice of basis) operation $\hat{\mathcal{E}}_1$ Eve can do on the travel qubit C can be written as

$$\hat{\mathcal{E}}_1 \left|\gamma\right\rangle_C \left|\epsilon\right\rangle_E = e \left|\gamma\right\rangle_C \left|\epsilon_{00}\right\rangle_E + f \left|\bar{\gamma}\right\rangle_C \left|\epsilon_{01}\right\rangle_E , \tag{7}$$

and

$$\hat{\mathcal{E}}_1 \left|\bar{\gamma}\right\rangle_C \left|\epsilon\right\rangle_E = e \left|\bar{\gamma}\right\rangle_C \left|\epsilon_{11}\right\rangle_E + f \left|\gamma\right\rangle_C \left|\epsilon_{10}\right\rangle_E , \tag{8}$$

where the states $|\epsilon_{00}\rangle$, $|\epsilon_{01}\rangle$, $|\epsilon_{11}\rangle$, and $|\epsilon_{10}\rangle$ of the ancilla E are normalized, but not orthogonal to each other. Without loss of generality, we can set $\langle\epsilon_{00}|\epsilon_{01}\rangle = \langle\epsilon_{00}|\epsilon_{10}\rangle = \langle\epsilon_{10}|\epsilon_{11}\rangle = \langle\epsilon_{01}|\epsilon_{11}\rangle = 0$, from the unitarity of $\mathcal{E}_1$[9].

The basis $\{|\gamma\rangle, |\bar{\gamma}\rangle\}$ for C is an arbitrary choice made by Eve. Recall that the angle α has

been chosen randomly for each travel qubit C and is never announced to the public; this is one of the biggest differences of our protocol both from the BB84-type and ping-pong-type protocols.

When $\langle\epsilon_{00}|\epsilon_{11}\rangle = \langle\epsilon_{01}|\epsilon_{10}\rangle = 1$, Eve cannot distinguish between $|\gamma\rangle_C$ and $|\bar{\gamma}\rangle_C$ by any measurement on her ancillae. In this case, Eve can acquire no more information than no attack is performed. Therefore, a minimal requirement for Eve's strategy is that such an operation as gives no information at all to her should not be detected by the legitimate partners (Alice and Bob). This can be achieved if Eve does not disturb travel qubits. It gives the condition, $|e| = 1$ and $|f| = 0$. In passing, we note that $\langle\epsilon_{00}|\epsilon_{11}\rangle = 0$ corresponds to an intercept-and-resend attack.

Having this ($|e| = 1$ and $|f| = 0$) in mind, we rewrite the attack operation on the travel qubit as

$$\hat{\mathcal{E}}_1 |\alpha_+\rangle_C = |\alpha_+\rangle_C \left(\cos^2\frac{\tilde{\alpha}}{2}|\epsilon_{00}\rangle + \sin^2\frac{\tilde{\alpha}}{2}|\epsilon_{11}\rangle\right) + i\sin\frac{\tilde{\alpha}}{2}\cos\frac{\tilde{\alpha}}{2}|\alpha_-\rangle_C (|\epsilon_{00}\rangle - |\epsilon_{11}\rangle) \quad (9)$$

and

$$\hat{\mathcal{E}}_1 |\alpha_-\rangle_C = -i\sin\frac{\tilde{\alpha}}{2}\cos\frac{\tilde{\alpha}}{2}|\alpha_+\rangle_C (|\epsilon_{00}\rangle - |\epsilon_{11}\rangle) + |\alpha_-\rangle_C \left(\sin^2\frac{\tilde{\alpha}}{2}|\epsilon_{00}\rangle + \cos^2\frac{\tilde{\alpha}}{2}|\epsilon_{11}\rangle\right), \quad (10)$$

where $\tilde{\alpha} \equiv \alpha - \gamma + \pi/2$.

On C's way from Bob back to Alice, Eve can perform another similar attack $\hat{\mathcal{E}}_2$ with a new ancilla F. With the same requirement as in $\hat{\mathcal{E}}_1$, the attack operation $\hat{\mathcal{E}}_2$ takes the simple form

$$\hat{\mathcal{E}}_2 |\gamma\rangle_C |\eta\rangle_F = |\gamma\rangle_C |\eta_{00}\rangle_F \quad (11)$$

and

$$\hat{\mathcal{E}}_2 |\bar{\gamma}\rangle_C |\eta\rangle_F = |\bar{\gamma}\rangle_C |\eta_{11}\rangle_F . \quad (12)$$

Since our protocol is symmetric between Alice and Bob, Eve's attack operations $\hat{\mathcal{E}}'_1$ and $\hat{\mathcal{E}}'_2$ on Bob's travel qubit D can be written, analogously to $\hat{\mathcal{E}}_1$ and $\hat{\mathcal{E}}_2$, with respect to new ancillae E' and F'. The optimal Eve's attack will be the symmetric one such that $\langle\epsilon_{00}|\epsilon_{11}\rangle = \langle\epsilon'_{00}|\epsilon'_{11}\rangle$

and $\langle\eta_{00}|\eta_{11}\rangle = \langle\eta'_{00}|\eta'_{11}\rangle$. The angle $\tilde{\beta} = \beta - \gamma + \pi/2$ relates Bob's choice $\{|\beta\rangle, |\bar{\beta}\rangle\}$ and Eve's choice $\{|\gamma\rangle, |\bar{\gamma}\rangle\}$ for the basis for D.

After all the procedures by Alice and Bob, Eve performs a collective measurement on her ancillae E, F, E', and F'. From the measurement result, she extracts the information about the state of Alice's home qubit A and Bob's B; namely, the information about the results of the QFR on the travel qubits C and D. The information is eventually the information about the key values shared by Alice and Bob.

The operations $\hat{\mathcal{E}}_1$, $\hat{\mathcal{E}}_2$, $\hat{\mathcal{E}}'_1$, and $\hat{\mathcal{E}}'_2$ by Eve inevitably disturb the quantum state of the travel qubit C and D. Simply comparing the test key bits (step 12 of the protocol), Alice and Bob may detect the attack. The detection probability p_d depends on the angle differences $\tilde{\alpha}$ and $\tilde{\beta}$. Since the angles $\tilde{\alpha}$ and $\tilde{\beta}$ are randomly distributed, the detection probability is given by

$$p_d = \frac{3}{8} - \frac{1}{8}\left(\cos^2 x + \cos^2 y + \cos^2 x \cos^2 y\right), \tag{13}$$

where $\cos x \equiv \langle\epsilon_{00}|\epsilon_{11}\rangle = \langle\epsilon'_{00}|\epsilon'_{11}\rangle$ and $\cos y \equiv \langle\eta_{00}|\eta_{11}\rangle = \langle\eta'_{00}|\eta'_{11}\rangle$. The maximum value of p_d is 3/8 corresponding to the intercept-and-resend attack($\cos x = \cos y = 0$).

Let us suppose that the initial state prepared by Alice and Bob is given by

$$|\Psi\rangle_i = |0\rangle_A |0\rangle_B |\alpha\beta\rangle_{CD}. \tag{14}$$

After all attacks the final state is given by

$$
\begin{aligned}
\frac{1}{2}\left|\alpha\beta\right\rangle_{CD}\Bigg\{&\frac{1}{4}\sin\tilde{\alpha}\sin\tilde{\beta}\left|\uparrow\uparrow\right\rangle_{AB}\left|1\right\rangle_{EF}\left|1'\right\rangle_{E'F'}+\left|\uparrow\downarrow\right\rangle_{AB}\left|5\right\rangle_{EF}\left|2'\right\rangle_{E'F'}\\
&+\left|\downarrow\uparrow\right\rangle_{AB}\left|2\right\rangle_{EF}\left|5'\right\rangle_{E'F'}+\frac{1}{4}\sin\tilde{\alpha}\sin\tilde{\beta}\left|\downarrow\downarrow\right\rangle_{AB}\left|4\right\rangle_{EF}\left|4'\right\rangle_{E'F'}\Bigg\}\\
+\frac{1}{2}\left|\alpha\bar{\beta}\right\rangle_{CD}\Bigg\{&-\frac{i}{2}\sin\tilde{\alpha}\left|\uparrow\uparrow\right\rangle_{AB}\left|1\right\rangle_{EF}\left|3'\right\rangle_{E'F'}-\frac{i}{2}\sin\tilde{\beta}\left|\uparrow\downarrow\right\rangle_{AB}\left|5\right\rangle_{EF}\left|1'\right\rangle_{E'F'}\\
&+\frac{i}{2}\sin\tilde{\beta}\left|\downarrow\uparrow\right\rangle_{AB}\left|2\right\rangle_{EF}\left|4'\right\rangle_{E'F'}+\frac{i}{2}\sin\tilde{\alpha}\left|\downarrow\downarrow\right\rangle_{AB}\left|4\right\rangle_{EF}\left|6'\right\rangle_{E'F'}\Bigg\}\\
\frac{1}{2}\left|\bar{\alpha}\beta\right\rangle_{CD}\Bigg\{&-\frac{i}{2}\sin\tilde{\beta}\left|\uparrow\uparrow\right\rangle_{AB}\left|3\right\rangle_{EF}\left|1'\right\rangle_{E'F'}+\frac{i}{2}\sin\tilde{\alpha}\left|\uparrow\downarrow\right\rangle_{AB}\left|4\right\rangle_{EF}\left|2'\right\rangle_{E'F'}\\
&-\frac{i}{2}\sin\tilde{\alpha}\left|\downarrow\uparrow\right\rangle_{AB}\left|1\right\rangle_{EF}\left|5'\right\rangle_{E'F'}+\frac{i}{2}\sin\tilde{\beta}\left|\downarrow\downarrow\right\rangle_{AB}\left|6\right\rangle_{EF}\left|4'\right\rangle_{E'F'}\Bigg\}\\
+\frac{1}{2}\left|\bar{\alpha}\bar{\beta}\right\rangle_{CD}\Bigg\{&-\left|\uparrow\uparrow\right\rangle_{AB}\left|3\right\rangle_{EF}\left|3'\right\rangle_{E'F'}+\frac{1}{4}\sin\tilde{\alpha}\sin\tilde{\beta}\left|\uparrow\downarrow\right\rangle_{AB}\left|4\right\rangle_{EF}\left|1'\right\rangle_{E'F'}\\
&+\frac{1}{4}\sin\tilde{\alpha}\sin\tilde{\beta}\left|\downarrow\uparrow\right\rangle_{AB}\left|1\right\rangle_{EF}\left|4'\right\rangle_{E'F'}-\left|\downarrow\downarrow\right\rangle_{AB}\left|6\right\rangle_{EF}\left|6'\right\rangle_{E'F'}\Bigg\} \qquad (15)
\end{aligned}
$$

with

$$\left|1\right\rangle_{EF}\equiv\left|\epsilon_{00}\right\rangle_{E}\left|\eta_{00}\right\rangle_{F}-\left|\epsilon_{11}\right\rangle_{E}\left|\eta_{11}\right\rangle_{F} \qquad (16)$$

$$\left|2\right\rangle_{EF}\equiv\sin^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{00}\right\rangle_{E}\left|\eta_{00}\right\rangle_{F}+\cos^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{11}\right\rangle_{E}\left|\eta_{11}\right\rangle_{F} \qquad (17)$$

$$\left|3\right\rangle_{EF}\equiv\cos^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{00}\right\rangle_{E}\left|\eta_{00}\right\rangle_{F}+\sin^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{11}\right\rangle_{E}\left|\eta_{11}\right\rangle_{F} \qquad (18)$$

$$\left|4\right\rangle_{EF}\equiv\left|\epsilon_{00}\right\rangle_{E}\left|\eta_{11}\right\rangle_{F}-\left|\epsilon_{11}\right\rangle_{E}\left|\eta_{00}\right\rangle_{F} \qquad (19)$$

$$\left|5\right\rangle_{EF}\equiv\cos^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{00}\right\rangle_{E}\left|\eta_{11}\right\rangle_{F}+\sin^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{11}\right\rangle_{E}\left|\eta_{00}\right\rangle_{F} \qquad (20)$$

and

$$\left|6\right\rangle_{EF}\equiv\sin^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{00}\right\rangle_{E}\left|\eta_{11}\right\rangle_{F}+\cos^{2}\frac{\tilde{\alpha}}{2}\left|\epsilon_{11}\right\rangle_{E}\left|\eta_{00}\right\rangle_{F} \qquad (21)$$

The states $\left|1'\right\rangle_{E'F'}$, $\left|2'\right\rangle_{E'F'}$, $\left|3'\right\rangle_{E'F'}$, $\left|4'\right\rangle_{E'F'}$, $\left|5'\right\rangle_{E'F'}$, and $\left|6'\right\rangle_{E'F'}$ are defined analogously (with $\tilde{\alpha}$ replaced by $\tilde{\beta}$).

Equation (15) clearly reveals how Eve can extract the information about the quantum state of the Alice's and Bob's home qubits A and B, respectively. For example, Eve can infer the state $\left|\uparrow\right\rangle_{B}$ on Bob's home qubit B if she finds her ancilla qubits E and F in the collective

state $|1\rangle_{EF}$, $|2\rangle_{EF}$, or $|3\rangle_{EF}$. Likewise, Eve infers the state $|\downarrow\rangle_B$ if she finds E and F in the state $|4\rangle_{EF}$, $|5\rangle_{EF}$, or $|6\rangle_{EF}$. The state of Alice's home qubit A can be inferred analogously from the ancillae E' and F'. The remaining question for Eve would be, for example, how to distinguish the states $|1\rangle_{EF}$, $|2\rangle_{EF}$, and $|3\rangle_{EF}$ from $|4\rangle_{EF}$, $|5\rangle_{EF}$, and $|6\rangle_{EF}$.

To this end, we first note that

$$\langle 1|4\rangle_{EF} = \langle 1|5\rangle_{EF} = \langle 1|6\rangle_{EF} = 0 \tag{22}$$

and that

$$\langle 4|1\rangle_{EF} = \langle 4|2\rangle_{EF} = \langle 4|3\rangle_{EF} = 0\,. \tag{23}$$

Therefore, Eve's best policy will be first to exploit the orthogonal subspaces containing $|1\rangle_{EF}$ and $|4\rangle_{EF}$, respectively, and then to distinguish the non-orthogonal states, namely $|2\rangle_{EF}$ and $|3\rangle_{EF}$ from $|5\rangle_{EF}$ and $|6\rangle_{EF}$, within these subspaces. Further, defining the normalized overlap

$$\overline{\langle i|j\rangle}_{EF} \equiv \frac{\langle i|j\rangle_{EF}}{\sqrt{\langle i|i\rangle_{EF}\,\langle j|j\rangle_{EF}}} \tag{24}$$

$(i, j = 1, \cdots, 6)$, we have the inequalities

$$\overline{\langle 2|5\rangle}_{EF} = \overline{\langle 3|6\rangle}_{EF} \geq \min\{\cos x, \cos y\} \tag{25}$$

and

$$\overline{\langle 2|6\rangle}_{EF} = \overline{\langle 3|5\rangle}_{EF} \geq \min\{\cos x, \cos y\} \tag{26}$$

Namely, the states $|2\rangle_{EF}$ and $|3\rangle_{EF}$ can be distinguished worse from $|5\rangle_{EF}$ and $|6\rangle_{EF}$ than any two states with the mutual overlap of $\min\{\cos x, \cos y\}$ can be distinguished from each other. Based on this observation, we analyze the worst case, where $\overline{\langle 2|5\rangle}_{EF} = \overline{\langle 3|6\rangle}_{EF} = \overline{\langle 2|6\rangle}_{EF} = \overline{\langle 3|5\rangle}_{EF} = \min\{\cos x, \cos y\}$. Further, it is clear that the optimal attack for Eve is the balanced one [9], for which $\cos x = \cos y$, and hereafter we focus on the balanced case.

Putting all the above observations together and with lengthy algebra, one can calculate the mutual information $I(A, B)$ between Alice and Bob and $I(A, E)$ [or $I(B, E)$] between Alice (or Bob) and Eve; note that because of the symmetry in our protocol, $I(A, E) = I(B, E)$. They are given by

$$I(A, B) = 1 + p_d \log_2 p_d + (1 - p_d) \log_2 (1 - p_d) \tag{27}$$

and

$$I(A, E) = 1 + p_e \log_2 p_e + (1 - p_e) \log_2 (1 - p_e)\,, \tag{28}$$

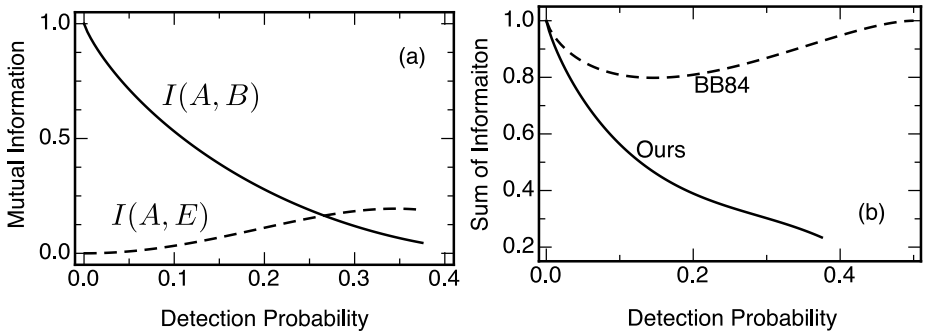

FIG. 4: (a) Mutual information a function of the detection probability, p_d, for general incoherent attacks against our protocol. The solid (dashed) line represents the mutual information $I(A,B)$ $[I(A,E)]$ between Alice and Bob (Alice and Eve). (b) $I(A,B)+I(A,E)$ as a function of p_d for our protocol (solid line) and for the BB84 protocol (dashed line). For our protocol, the maximum value of p_d is 3/8.

respectively. p_d in Eq. (27) is the detection probability [see Eq. (13)] for the balanced attack ($\cos x = \cos y$), and p_e in Eq. (28) is defined by

$$p_e = \frac{1}{2} - \frac{1}{2}\sqrt{1-2p_d}(1-\sqrt{1-2p_d})\left[2\sqrt{1-2p_d}+\sqrt{2(1-\sqrt{1-2p_d})}\right]. \qquad (29)$$

For a QKD to be secure, it is required that $I(A,B) \geq I(A,E)$[5]. The mutual information $I(A,B)$ and $I(A,E)$ are plotted as functions of the detection probability p_d in Fig. 4. The maximum information between Alice and Eve occurs at $p_d = 0.345$, which is less than the maximum detection probability ($p_d = 3/8$) corresponding to the intercept-and-resend attack. This means that the intercept-and-resend attack is not an optimal attack for Eve. $I(A,B)$ and $I(A,E)$ becomes equal for the detection probability $p_d = 0.266188$. This detection probability is greater than $p_d = 0.18$ for the ping-pong protocol [9] and $p_d = 0.15$ for BB84 protocol.

So far the security has been analyzed for incoherent attacks. In general, Eve can attacks many qubits coherently by collecting many ancillae and performing a global measurement on them. Since our protocol shares many common features with the BB84 or similar protocols, we can first follow the lines in Section VI.G of Ref. [5] to prove the security of our protocol against collective attacks[12]. An argument for the security against the most general coherent attacks[13] is given below. After Alice and Bob repeats the protocol n times to share a key of length of $2n$ bits, the sum of the mutual information $I(A,B)$ and $I(A,E)$ should be less

than $2n$, i.e.,

$$I(A,B) + I(A,E) \leq 2n\,. \tag{30}$$

Equivalently speaking, $I(A,B) + I(A,E) \leq 1$ per single qubit. This is because Eve and Bob cannot acquire more information than is sent out mutually by Alice and Bob whatever measurement is performed by Eve. Therefore, in order that $I(A,B) > I(A,E)$ (Theorem 1 in Ref. [5]), it suffices to have $I(A,B) \geq n$. Since $I(A,B) = 2n\left[1 + p_d \log_2 p_d + (1-p_d)\log_2(1-p_d)\right]$, p_d is required to be less than 0.110028, approximately 11 %, which is the upper bound for the BB84 protocol[12, 13]. This proves that our protocol is *at least* as secure as the BB84 protocol against collective attacks. The above lines of proof applies only for collective attacks. However, it has been argued that the collective attack may be the optimal one of the most general coherent attacks[14]. It is also interesting to note that for incoherent attacks, $I(A,E)$ in Eq. (28) is significantly restricted and hence the sum $I(A,B) + I(A,E)$ per single qubit is far less than 1; cf. (30). This is demonstrated in Fig. 4 (b) comparing the sum for the BB84 protocol and for ours. It suggest that the upper bound $p_d \approx 11$ % may be reduced further with proper analysis of the restriction on the possible measurements by Eve. More detailed analysis of the security of our protocol against the coherent attacks should therefore be an interesting topic for further studies in the future.

IV. IMPERSONATION ATTACK

In our protocol, Alice sends a qubit to Bob and gets it back. So does Bob with another travel qubit. It is possible for Eve to intercept the channel and pretend to be her/his legitimate partner to each. One can think of two different ways of impersonation attack. In the first method [see Fig. 5(a)], Eve uses two home qubits of her own. Eve can use one of the two to share a perfect key with Alice following the procedures of the protocol in Section II, and the other to share another key with Bob. However, the keys so generated to Alice and Bob are independent and have no correlation. Therefore, by bit verification procedure, this attack can be detected with probability 1/2.

In the second method [see Fig. 5(b)], Eve uses only one home qubit E of her own, which is used for the interaction with both Alice and Bob. In this case, the total wave function of

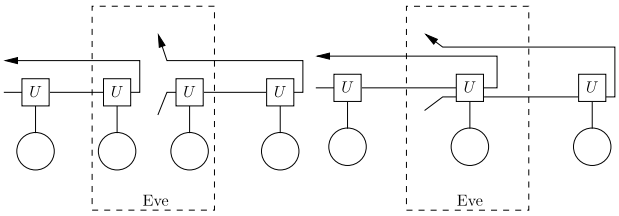

FIG. 5: Impersonation attack

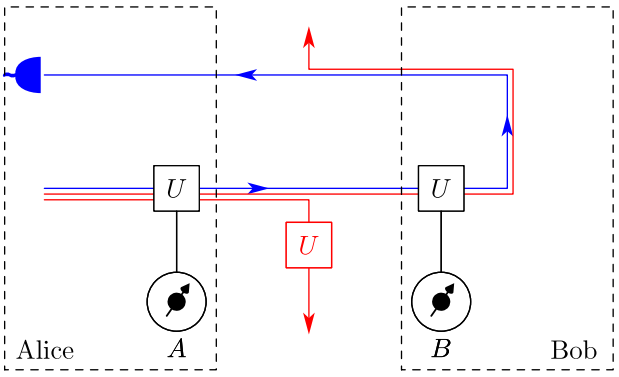

FIG. 6: Photon-number splitting attack.

the whole qubits is given by

$$(|\uparrow\uparrow\uparrow\rangle + |\downarrow\downarrow\downarrow\rangle)\left|\bar{\alpha}\bar{\beta}\bar{\epsilon}\right\rangle + (|\uparrow\downarrow\uparrow\rangle + |\downarrow\uparrow\downarrow\rangle)\left|\bar{\alpha}\beta\bar{\epsilon}\right\rangle + (|\uparrow\uparrow\downarrow\rangle + |\downarrow\downarrow\uparrow\rangle)\left|\alpha\beta\epsilon\right\rangle + (|\uparrow\downarrow\downarrow\rangle + |\downarrow\uparrow\uparrow\rangle)\left|\alpha\bar{\beta}\epsilon\right\rangle \quad (31)$$

(not normalized), where the product states are arranged such as $|...\rangle_{ABE}\,|...\rangle_{CDE'}$ (E' is the travel qubit of Eve's). It then follows immediately that the detection probability of this attack is still 1/2.

V. PHOTON NUMBER SPLITTING ATTACK

Finally, we investigate the security of the protocol against the photon number splitting attack (PNS). (We note that the security analysis in the case of lossy channel is essentially the same as that against the PNS attack.) Let us suppose that the photon source generate three photons (the discussion can be trivially generalized to the case of more photons; see below). Eve takes one photon (say E_1) on the quantum channel from Alice to Bob and another (E_2) on the channel back to Alice from Bob; see Fig. 6. Only photon C finally arrives at Alice's hand. Similarly, Eve takes photons E_1' and E_2' out of the photons from

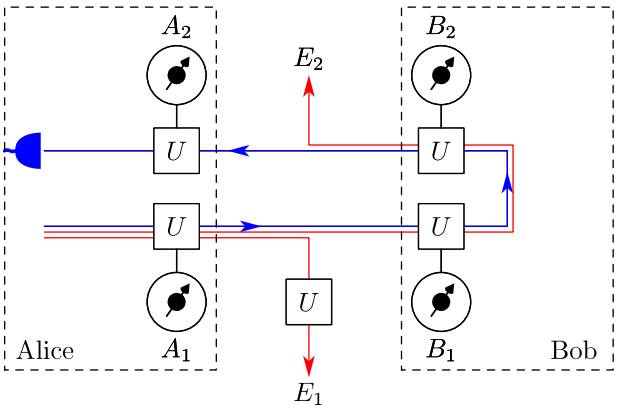

FIG. 7: (color on-line) A variation of the protocol using four home qubits.

Bob. Bob receives back only D. The final state of the whole photons and home qubits are given by

$$i\left|\uparrow\uparrow\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle - i\left|\downarrow\downarrow\right\rangle\left|\alpha\beta\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle + \left|\uparrow\downarrow\right\rangle\left|\bar{\alpha}\beta\right\rangle\left|\alpha\beta\right\rangle\left|\alpha\beta\right\rangle + \left|\downarrow\uparrow\right\rangle\left|\alpha\bar{\beta}\right\rangle\left|\alpha\beta\right\rangle\left|\alpha\beta\right\rangle , \quad (32)$$

where the product states have been denoted according to the arrangement of the qubits such as $\left|..\right\rangle_{AB}\left|..\right\rangle_{E_1E_2}\left|..\right\rangle_{E_1'E_2'}\left|..\right\rangle_{CD}$. Eve waits until Alice and Bob performs projective measurement on their travel qubits C and D. Then the wave function in Eq. (32) collapses into either

$$\left|\uparrow\uparrow\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle - \left|\downarrow\downarrow\right\rangle\left|\alpha\beta\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle\left|\bar{\alpha}\bar{\beta}\right\rangle \quad (33)$$

or

$$\left|\uparrow\downarrow\right\rangle\left|\bar{\alpha}\beta\right\rangle\left|\alpha\beta\right\rangle\left|\alpha\beta\right\rangle + \left|\downarrow\uparrow\right\rangle\left|\alpha\bar{\beta}\right\rangle\left|\alpha\beta\right\rangle\left|\alpha\beta\right\rangle . \quad (34)$$

Therefore, Eve can know the key without being detected simply by checking whether $\langle\epsilon_1|\epsilon_2\rangle\langle\epsilon_1'|\epsilon_2'\rangle > 0$ (Alice and Bob share the key 0) $\langle\epsilon_1|\epsilon_2\rangle\langle\epsilon_1'|\epsilon_2'\rangle < 0$ (Alice and Bob share the key 1), where $\epsilon_1, \epsilon_1' = \alpha, \bar{\alpha}$ and $\epsilon_2, \epsilon_2' = \beta, \bar{\beta}$. This test can be easily done, for example, using an interferometer. The discuss is trivially generalized to the case of even more photons. It is enough for Eve to steal two photons from Alice and another two from Bob.

One may be tempted to overcome this problem using four home qubits (two for Alice and two for Bob) as illustrated in Fig. 7. This scheme "hides" by means of entanglement the output state of C and D even after Alice and Bob performs projective measurements on C and D. However, following the similar lines as above, the total wave function of the whole qubits is given by

$$
\begin{aligned}
&-\frac{1}{4}\left|\bar{\alpha}\bar{\beta}\right\rangle\left(\left|\Phi^{+}\Psi^{+}\right\rangle\left|\Phi^{+}\Psi^{+}\right\rangle+\left|\Phi^{+}\Psi^{-}\right\rangle\left|\Phi^{+}\Psi^{-}\right\rangle-\left|\Phi^{-}\Psi^{+}\right\rangle\left|\Phi^{-}\Psi^{+}\right\rangle-\left|\Phi^{-}\Psi^{-}\right\rangle\left|\Phi^{-}\Psi^{-}\right\rangle\right)\\
&-\frac{1}{4}\left|\bar{\alpha}\bar{\beta}\right\rangle\left(\left|\Psi^{-}\Phi^{-}\right\rangle\left|\Psi^{+}\Phi^{+}\right\rangle-\left|\Psi^{-}\Phi^{+}\right\rangle\left|\Psi^{+}\Phi^{-}\right\rangle+\left|\Psi^{+}\Phi^{-}\right\rangle\left|\Psi^{-}\Phi^{+}\right\rangle-\left|\Psi^{+}\Phi^{+}\right\rangle\left|\Psi^{-}\Phi^{-}\right\rangle\right)\\
&-\frac{i}{4}\left|\alpha\beta\right\rangle\left(\left|\Psi^{-}\Psi^{+}\right\rangle\left|\Phi^{+}\Phi^{+}\right\rangle-\left|\Psi^{-}\Psi^{-}\right\rangle\left|\Phi^{+}\Phi^{-}\right\rangle-\left|\Psi^{+}\Psi^{+}\right\rangle\left|\Phi^{-}\Phi^{+}\right\rangle+\left|\Psi^{+}\Psi^{-}\right\rangle\left|\Phi^{-}\Phi^{-}\right\rangle\right)\\
&+\frac{i}{4}\left|\alpha\beta\right\rangle\left(\left|\Phi^{+}\Phi^{-}\right\rangle\left|\Psi^{+}\Psi^{+}\right\rangle+\left|\Phi^{+}\Phi^{+}\right\rangle\left|\Psi^{+}\Psi^{-}\right\rangle+\left|\Phi^{-}\Phi^{-}\right\rangle\left|\Psi^{-}\Psi^{+}\right\rangle+\left|\Phi^{-}\Phi^{+}\right\rangle\left|\Psi^{-}\Psi^{-}\right\rangle\right) \quad (35)
\end{aligned}
$$

arranging the product states such as $\left|..\right\rangle_{CD}\left|..\right\rangle_{A_1A_2B_1B_2}\left|..\right\rangle_{E_1E_2E_1'E_2'}$ Therefore, in order to know the key, all Eve has to do is to distinguish the Bell state $\left|\Phi^{\pm}\right\rangle$ from $\left|\Psi^{\pm}\right\rangle$, which is as easy as the test for the two-home-qubit scheme analyzed above.

VI. EXPERIMENTAL FEASIBILITY

The parametric Faraday rotation of photon polarization by atomic spins have been widely used in quantum optics and atomic physics. For example, it has been used for quantum non-demolition measurement of the atomic spin[15, 16, 17]. However, because of the weak atom-photon interaction, the Faraday rotation angle is usually quite small (several degrees). To enhance the atom-photon interaction to achieve the rotation angle of $\pi/2$, one has to put an atom to a cavity. However, trapping a single atom in a cavity is still technologically challenging.

Another candidate for a conditional Faraday rotation of photon polarization is the quantum dot in a micro-cavity, which has already been demonstrated experimentally[18, 19]. Here the photon interacts with the electron spin in the semiconductor quantum dot. The transmission distance is limited mainly by the coherence time of the electron spin in the quantum dot. The maximum transmission distance (given by the speed of light) would be 10 m and 1×10^6 m for coherence times of 100 ns [20] and for 10 ms [21] in one-way transmission. We believe the distance limitation will be extensively relaxed in the near future.

VII. CONCLUSION

We have proposed a new QKD protocol exploring the quantum states of the Faraday rotators. The protocol is secure against eavesdropping for ideal single-photon source and

robust against impersonation attacks. This protocol is not allowed for multiphoton source which produces more than two photons. The protocol could be implemented experimentally with semiconductor quantum dots in micro-cavity.

Acknowledgments

We thank J. W. Lee and B.-G. Englert for helpful discussions. This work was supported by the SRC/ERC program of MOST/KOSEF (R11-2000-071), the Korea Research Foundation Grants (KRF-2005-070-C00055 and KRF-2006-312-C00543), the SK Fund, and the KIAS.

---

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, CA, 1994), p. 124.

[2] C. H. Bennett and G. Brassard (IEEE Press, New York, 1984), pp. 175–179.

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] C. H. Bennett, G. Brassard, and A. Ekert, Sci. Am. **267**, 50 (1992).

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinde, Rev. Mod. Phys. **74**, 145 (2002).

[6] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187 902 (2002).

[7] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).

[8] Q.-Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).

[9] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).

[10] The initial preparation of $|\phi = 0\rangle$ of QFR is just for convenience. The initial state of QFR is required to be an arbitrary state on the equator of the Poincaré sphere.

[11] Yet a classical channel is necessary at the key verification state in order to detect possible eavesdropping.

[12] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[13] C. R. Mayers and J. S. Langer, Phys. Rev. E **47**, 3048 (1993).

[14] See, e.g., R. Renner, arXiv:quant-ph/0512258v2; J. Bae and A. Acin, arXiv:quant-ph/0610048v1; R. Renner, arXiv:quant-ph/0703069v1.

[15] M. Kitagawa and M. Ueda, Phys. Rev. A **47**, 5138 (1993).

[16] D. J. Wineland, J. J. Bollinger, W. M. Itano, F. L. Moore, and D. J. Heinzen, Phys. Rev. A **46**, 6797 (1992).

[17] A. Kuzmich, L. Mandel, and N. P. Bigelow, Phys. Rev. Lett. **85**, 1594 (2000).

[18] A. Imamoḡlu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, Phys. Rev. Lett. **83**, 4204 (1999).

[19] M. N. Leuenberger, M. E. Flatté, and D. D. Awschalom, Phys. Rev. Lett. **94**, 107401 (2005).

[20] J. M. Kikkawa and D.D. Awschalom, Phys. Rev. Lett. **80**, 4313 (1998).

[21] M. Kroutvar *et al.*, Nature (London) **432**, 81 (2004).